

REMARKS

Applicants respectfully traverse and request reconsideration.

Applicants also wish to thank the Examiner for the notice that Claims 6-9, 13-17 and 45-47 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 1-5, 10, 12, 18, 19, 23, 24, 27, 32, 33, 35-37 and 40-44 stand rejected under 35 U.S.C. §102(b) as being anticipated by Appelbaum (U.S. Patent No. 4,683,968). Appelbaum is directed to a system which enables a protected program to run on only a selected plurality of computers wherein a computer and memory has stored thereon encrypted programs. A unique key K_i is used for each computer and each key is triple encrypted repeatedly using a fixed key KFK. A special module which also contains the unique key is connected to the computer. The computer also includes a checker program that responds to a request to use a protected program. As such, the computer, through the checker program, first performs a single decryption procedure on the triple encrypted key and sends the remaining result to the module as a message. As such, the module (third party) does not receive the triple encrypted key but to the contrary, receives a partially decrypted encrypted key since the single decryption was already performed by the computer (second party). The module (third party) then performs another single decryption procedure using the unique key K_i on the message and sends the result back to the computer. The computer receives the message and performs another decryption procedure using the same fixed key KFK as it previously used the first time it performed single decryption. The checker program then obtains the unique key to decrypt an identifier and proceeds with the execution of the protected program only if it is identified by the decrypted identifier. As such, it appears that the computer (second party) performs the same decryption operation using the same decryption key twice and another unit performs a decryption operation using the unique key.

The Office Action equates the claimed double key package to the triple encrypted key set forth in the Appelbaum reference. In addition, the Office Action equates the computer to the claimed second party and equates the module to the claimed third party. It does not appear that the Office Action addresses which entity is the claimed first party. As such, Applicants respectfully request such a showing if the rejection is maintained.

In any event, the Appelbaum system does not anticipate the above claims for several reasons. For example, the claims require that the third party receives the double key package as communicated by the second party. However, taking the Office Action's corresponding elements from the reference, it is evident that the module (third party) of the Appelbaum reference does not receive the double key package as required by the claim. To the contrary, the second party (the computer) first performs a first decryption procedure prior to sending the alleged double key package to the module (third party). This is in contrast to Applicants' claimed invention which requires, among other things, communicating, by the second party, the double key package, as provided by the first party, to the third party. As such, the claims are in condition for allowance for this reason alone.

Moreover, the claims require a recovery of a decryption key for the second party using a third party based decryption key. This is taught by the cited reference because the computer of Appelbaum only appears to utilize a single decryption key, namely the fixed key FK. As claimed, the operation must require, for example, the recovery of a decryption key for a second party. However, the alleged second party (the computer) of Appelbaum does not obtain a recovered key from the module but already has the key FK. Accordingly, there is no recovery of a decryption key by computer of Appelbaum as set forth in Applicants' claims. As such, the claims are in condition for allowance.

In addition, the dependent claims add additional novel and nonobvious subject matter. For example, claims 2, 3 and 4 refer to the recovery of a decryption key that is communicated to the second party which is not described in Appelbaum. In addition, there is no double application of an asymmetric public key encryption as required by the claims since a fixed key approach appears to be used. Moreover, as noted in claim 4, there is no combination of symmetric key and double application of an asymmetric public key encryption wherein there is a public key associated with a second party and a public key associated with a third party as claimed. As such, these claims are also in condition for allowance. In addition, claim 5 also includes encrypting the first key package using a third encryption key associated with the third party to produce the double key package. There does not appear to be any third encryption key in Appelbaum since it appears to describe two keys, namely key FK and key Ki. As such, these claims are also in condition for allowance. Applicants respectfully reassert the same remarks with respect to corresponding dependent claims.

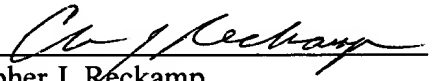
Claims 11, 25, 26, and 31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Appelbaum in view of Perlman. Applicants respectfully reassert the relevant remarks made above and as such these claims are also in condition for allowance.

Claims 20-22, 28-30, 38, 39 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Appelbaum in view of U.S. Patent No. 5,920,630. Applicants respectfully reassert the relevant remarks made above with respect to the Appelbaum reference and as such these claims are also in condition for allowance. In addition, Applicants respectfully note that even combining the Wertheimer reference with that of Appelbaum would not result in Applicants' claimed invention. For example, as noted above, there is no teaching in Appelbaum of the third party based encrypted security token nor of the double key package being

communicated as required in the claims. In addition, using Wertheimer and combining selected teachings with Appelbaum would likely result in simply having the signed triple encrypted key of Appelbaum sent to the computer. There is no teaching or suggestion of producing a signed message with a third party based encrypted security token. As such, these claims are also in condition for allowance.

Accordingly, Applicants respectfully submit that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

By: 
Christopher J. Reckamp
Registration No. 34,414

Date: December 3, 2003
Vedder, Price, Kaufman & Kammholz, P.C.
222 N. LaSalle Street
Chicago, IL 60601
Telephone: (312) 609-7599
Facsimile: (312) 609-5005
Email: creckamp@vedderprice.com